



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/605,173	09/12/2003	ASHOT ANDREASYAN	PR 1803.01 US	2172

31883 7590 03/11/2010  
DVA/PIONEER RESEARCH CENTER USA, INC.  
2265 E. 220TH STREET  
LONG BEACH, CA 90810

EXAMINER
----------

TRUVAN, LEYNNA THANH

ART UNIT	PAPER NUMBER
----------	--------------

2435

MAIL DATE	DELIVERY MODE
-----------	---------------

03/11/2010

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/605,173	<b>Applicant(s)</b> ANDREASYAN, ASHOT	
	<b>Examiner</b> Leynna T. Truvan	<b>Art Unit</b> 2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 14 December 2009.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 36-39 and 41-63 is/are pending in the application.
- 4a) Of the above claim(s) 1-35 and 40 is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 36-39 and 41-63 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |   |   |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                    | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)         | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____   | 6) <input type="checkbox"/> Other: _____                          |

### **DETAILED ACTION**

1. Claims 36-39 and 41-63 are now pending.  
Claims 1-35 and 40 are cancelled by applicant.

### ***Response to Arguments***

2. Applicant's arguments filed 12/14/2009 have been fully considered but they are not persuasive.

Regarding claim 36, applicant's argument on pg.8 that there is nothing in Immonen about generating a shared secret key with a public key of a certificate. Immonen discloses verifying the certificate, obtains the public key and calculates the shared secret key. Immonen also discloses it is preferable to use the public key handshake only for exchanging parameters which are used for computing a shared key for symmetric cryptography (col.4, lines 2-6). Thus, when the shared secret key is generated the public key is included with the verified certificate which reads on the claimed with the public key (col.3, lines 16-27).

Regarding claim 36, applicant's argument on pg.9 that Moharram does not teach or expressly or impliedly suggest all the elements of claim 36. Moharram is the secondary art which is not required to teach all the elements of claim 36 but suggests similar attributes and systems as the primary art Immonen. Immonen is the primary art

Art Unit: 2435

to disclose “generating a second shared secret key for the first peer” and Moharram is combined with Immonen to teach “with the second public key from the second peer and a private key of the first peer”. Moharram discloses the consumer (1<sup>st</sup> peer) obtains a digital certificate that contains the consumer’s public key that is sent to peer (2<sup>nd</sup> peer) and computes a shared secret key (col.9, lines 30-33). Moharram discloses computing the shared secret key from peer’s public key and owner private key where owner is referring to the consumer (1<sup>st</sup> peer) (col.9, lines 36-45). It would have been obvious for a person of ordinary skills in the art at the time of the invention to modify Immonen to teach generating a 2<sup>nd</sup> shared secret key for the 1<sup>st</sup> peer with the 2<sup>nd</sup> public key from the 2<sup>nd</sup> peer and a private key of the 1<sup>st</sup> peer because this shows that the claimed 1<sup>st</sup> and 2<sup>nd</sup> shared secret key are two separate different shared secret keys that are not generated the same as one another and verifies the parties’ identities which certifies the key is his/her own (Moharram-col.9, lines 6-35). Thus, the Immonen and Moharram combination reads on the claimed invention.

Regarding claim 63, applicant stated on pg.9 recites limitations of claim 36 and additionally includes “wherein generating the first shared secret key for the second peer with the first public key of the first certificate is carried out independently of any public key generated by the first peer and the second peer”. Applicant argues this limitation saves a step of Diffie-Hellman algorithm which is in contrast to the teachings of Immonen. Immonen gives many different algorithms that are known in the computer technology and uses an effective overhead of the handshake protocol according to the

Art Unit: 2435

invention is only two inter-party messages compared to an overhead of four messages in the prior art handshake (col.3, lines 35-40). By generating the shared secret key of the first certificate is known prior art and is carried out independently of any public key generated by the first peer and second peer does not contrast to Immonen's invention and this limitation does not suggest saving step. For the generated shared secret key of the first certificate is known to be independent of the keys (public) of the peers because the certificate derives from a certifying authority (CA) versus the public keys are from the peers themselves used to match/verify with the CA. Additionally, Immonen discloses each party independently calculates a shared secret key and then exchanges them for verification of identity of the other party (col.1, lines 56-60). By means of certificates signed by a mutually trusted authority, each party can verify its peer's identity (col.1, lines 62-65). Immonen also discloses it is preferable to use the public key handshake only for exchanging parameters which are used for computing a shared key for symmetric cryptography (col.4, lines 2-6). Immonen is the primary art to disclose "generating a second shared secret key for the first peer" and Moharram makes up the deficiency of the claimed "with the second public key from the second peer and a private key of the first peer". Thus, the Immonen and Moharram combination reads on claim 63.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**3. Claims 36-39 and 41-63 are rejected under 35 U.S.C. 103(a) as being unpatentable over Immonen (US 6,931,528) in view of Moharram, et al. (US 7,290,286).**

**As per claim 36:**

Immonen discloses the method for generating shared keys comprising:  
providing a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters that comprises a first public key for the first peer;  
**(col.1, lines 48-51; 1<sup>st</sup> peer is in form of server B)**

generating a second public key by the second peer with at least one parameter of the plurality of first parameters and a first private key of the second peer; **(col.1, lines 54-55 and col.1, line 64-col.2, line 5; 2<sup>nd</sup> peer is in form of client A)**

providing the generated second public key from the second peer to the first peer;  
**(col.1, lines 54-55 and col.3, lines 16-25)**

generating a first shared secret key for the second peer with the first public key of the first certificate; and **(col.1, lines 57-60 and col.3, lines 23-26)**

generating a second shared secret key for the first peer [*with the second public key from the second peer and a private key of the first peer*]. **(col.1, lines 57-60 and col.3, lines 16-19)**

Immonen discloses each party (i.e. 1<sup>st</sup> & 2<sup>nd</sup> peers) independently calculates a shared secret key where client A (2<sup>nd</sup> peer) obtains server B's public key (of 1<sup>st</sup> certificate) to calculate a (1<sup>st</sup>) shared secret key (col.1, lines 57-60 and col.3, lines 23-26). Immonen also calculates the same process for the (2<sup>nd</sup>) shared secret key for server B (1<sup>st</sup> peer) so that each party can verify its peer's identity. Thus, Immonen includes a 1<sup>st</sup> shared secret key for the 2<sup>nd</sup> peer and a 2<sup>nd</sup> shared secret key for the 1<sup>st</sup> peer. However, Immonen does not include the 2<sup>nd</sup> shared secret key is generated with the 2<sup>nd</sup> public key from the 2<sup>nd</sup> peer and a private key of the 1<sup>st</sup> peer.

To simplify terminology from one art to another that corresponds to the claimed invention, is referred in the rejection as follows:

**First peer (1<sup>st</sup> peer) = Server B (Immonen) = Consumer/owner (Moharram)**

**Second peer (2<sup>nd</sup> peer) = Client A (Immonen) = Peer (Moharram)**

Moharram discloses the consumer (1<sup>st</sup> peer) obtains a digital certificate that contains the consumer's public key that is sent to peer (2<sup>nd</sup> peer) and computes a shared secret key (col.9, lines 30-33). Moharram discloses computing the shared secret key from peer's public key and owner private key where owner is referring to the consumer (1<sup>st</sup> peer) (col.9, lines 36-45). Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to modify Immonen to teach generating a 2<sup>nd</sup> shared secret key for the 1<sup>st</sup> peer with the 2<sup>nd</sup> public key from

the 2<sup>nd</sup> peer and a private key of the 1<sup>st</sup> peer because this shows that the claimed 1<sup>st</sup> and 2<sup>nd</sup> shared secret key are two separate different shared secret keys that are not generated the same as one another and verifies the parties' identities which certifies the key is his/her own (Moharram-col.9, lines 6-35).

**As per claim 37: See Immonen on col.1, lines 47-67 and col.3, lines 23-45;**

discussing the method of claim 36 and further comprising providing a second certificate from the second peer to the first peer, the second certificate comprising a plurality of second parameters.

**As per claim 38: See Moharram on col.9, lines 27-50;** discussing the method of claim 37 wherein generating the second shared secret key for the first peer with the second public key from the second peer and a private key of the first peer further comprises generating the second shared secret key for the first peer with the second public key from the second peer, the private key of the first peer and at least one of the plurality of second parameters.

**As per claim 39: See Immonen on col.1, lines 47-67 and col.3, lines 23-26 and Moharram on col.9, lines 27-50;** discussing the method of claim 36 wherein the first public key of the first certificate is received from a third party certificate authority.

**As per claim 41: See Immonen on col.3, lines 1-5 and Moharram on col.9, lines 27-50;** discussing the method of claim 36 wherein the plurality of first parameters of the first certificate comprises at least one prime number and at least one generator in addition to the first public key of the first certificate.



**As per claim 42:** See Immonen on col.4, lines 1-5; discussing the method of claim 37 wherein the plurality of second parameters of the second certificate comprises at least one prime number, at least one generator and a public key of the second certificate that is received from a third party certificate authority.

**As per claim 43:** See Immonen on col.3, lines 23-26 and Moharram on col., lines; discussing the method of claim 42 and wherein the generating a second shared secret key for the first peer with the second public key from the second peer and a private key of the first peer is carried out without employing either the first public key of the first certificate or the public key of the second certificate.

**As per claim 44:** See Immonen on col.4, lines 1-5; discussing the method of claim 37 wherein both the first certificate including the plurality of first parameters and the second certificate including the plurality of second parameters are generated independently of the first peer and the second peer.

**As per claim 45:** See Immonen on col.3, lines 44-45; discussing the method of claim 37 wherein both the first certificate and the second certificate comprise Digital Signature Algorithm (DSA) type certificates.

**As per claim 46:** See Immonen on col.3, lines 43-45; discussing the method of claim 37 wherein the plurality of first parameters and the plurality of second parameters comprise digital signature standard parameters.

**As per claim 47:** See Immonen on col.4, lines 44-52; discussing the method of claim 37 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

**As per claim 48:** See Immonen on col.4, lines 41-50; discussing the method of claim 36 wherein the first peer and the second peer communicate over a network.

**As per claim 49:** See Immonen on col.4, lines 44-52; discussing the method of claim 48 wherein the network comprises at least one of a wireless network or a Bluetooth network.

**As per claim 50:** See Immonen on col.1, lines 47-67 and col.3, lines 23-26; discussing the method of claim 36 wherein the first public key of the first certificate is a variable used in the step of generating the first shared key.

**As per claim 51:**

Immonen discloses the system comprising:  
a processor; and a memory coupled to the processor,  
the memory containing program code that, when executed by the processor,  
causes the processor to:  
provide a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters that comprises a first public key for the first peer;  
**(col.1, lines 48-51; 1<sup>st</sup> peer is in form of server B)**

generate a second public key by the second peer with at least one parameter of the plurality of first parameters and a first private key of the second peer; **(col.1, lines 54-55 and col.1, line 64-col.2, line 5; 2<sup>nd</sup> peer is in form of client A)**

provide a second certificate and the second public key from the second peer to the first peer, the second certificate comprising a plurality of second parameters; **(col.1, lines 54-55 and col.3, lines 16-25)**

generate a first shared secret key for the second peer with the first public key of the first certificate; and **(col.1, lines 57-60 and col.3, lines 23-26)**

generate a second shared secret key for the first peer [*with the second public key from the second peer, a private key from of first peer and at least one of the plurality of second parameters*]. **(col.1, lines 57-60 and col.3, lines 16-19)**

Immonen discloses each party (i.e. 1<sup>st</sup> & 2<sup>nd</sup> peers) independently calculates a shared secret key where client A (2<sup>nd</sup> peer) obtains server B's public key (of 1<sup>st</sup> certificate) to calculate a (1<sup>st</sup>) shared secret key (col.1, lines 57-60 and col.3, lines 23-26). Immonen also calculates the same process for the (2<sup>nd</sup>) shared secret key for server B (1<sup>st</sup> peer) so that each party can verify its peer's identity. Thus, Immonen includes a 1<sup>st</sup> shared secret key for the 2<sup>nd</sup> peer and a 2<sup>nd</sup> shared secret key for the 1<sup>st</sup> peer. However, Immonen does not include the 2<sup>nd</sup> shared secret key is generated with the 2<sup>nd</sup> public key from the 2<sup>nd</sup> peer and a private key of the 1<sup>st</sup> peer.

To simplify terminology from one art to another that corresponds to the claimed invention, is referred in the rejection as follows:

**First peer (1<sup>st</sup> peer) = Server B (Immonen) = Consumer/owner (Moharram)**

**Second peer (2<sup>nd</sup> peer) = Client A (Immonen) = Peer (Moharram)**

Moharram discloses the consumer (1<sup>st</sup> peer) obtains a digital certificate that contains the consumer's public key that is sent to peer (2<sup>nd</sup> peer) and computes a shared secret key (col.9, lines 30-33). Moharram discloses computing the shared secret key from peer's public key and owner private key where owner is referring to the consumer (1<sup>st</sup> peer) (col.9, lines 36-45). Therefore, it would have been obvious for a

person of ordinary skills in the art at the time of the invention to modify Immonen to teach generating a 2nd shared secret key for the 1<sup>st</sup> peer with the 2<sup>nd</sup> public key from the 2<sup>nd</sup> peer and a private key of the 1<sup>st</sup> peer because this shows that the claimed 1<sup>st</sup> and 2<sup>nd</sup> shared secret key are two separate different shared secret keys that are not generated the same as one another and verifies the parties' identities which certifies the key is his/her own (Moharram-col.9, lines 6-35).

**As per claim 52: See Immonen on col.1, lines 47-67 and col.4, lines 1-5;**

discussing the system of claim 51 wherein both the first certificate including the plurality of first parameters and the second certificate including the plurality of second parameters are generated independently of the first peer and the second peer.

**As per claim 53: See Immonen on col.3, lines 44-45;** discussing the system of claim 51 wherein both the first certificate and the second certificate comprise Digital Signature Algorithm (DSA) type certificates.

**As per claim 54: See Immonen on col.3, lines 43-45;** discussing the system of claim 51 wherein the plurality of first parameters and the plurality of second parameters comprise digital signature standard parameters.

**As per claim 55: See Immonen on col.4, lines 44-52;** discussing the system of claim 51 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

**As per claim 56: See Immonen on col.4, lines 44-52;** discussing the system of claim 51 wherein the first peer and the second peer communicate over a network that comprises at least one of a wireless network or a Bluetooth network.

**As per claim 57:**

Immonen discloses a computer storage medium including data that, when accessed by a computer, causes the computer to perform operations comprising:

providing a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters that comprises a first public key for the first peer;

**(col.1, lines 48-51; 1<sup>st</sup> peer is in form of server B)**

generating a second public key by the second peer with at least one parameter of the plurality of first parameters and a first private key of the second peer; **(col.1, lines 54-55 and col.1, line 64-col.2, line 5; 2<sup>nd</sup> peer is in form of client A)**

providing a second certificate and the second public key from the second peer to the first peer, the second certificate comprising a plurality of second parameters; **(col.1, lines 54-55 and col.3, lines 16-25)**

generating a first shared secret key for the second peer with the first public key of the first certificate; and **(col.1, lines 57-60 and col.3, lines 23-25)**

generating a second shared secret key for the first peer [*with the second public key from the second peer, a private key from of first peer and at least one of the plurality of second parameters*]. **(col.1, lines 57-60 and col.3, lines 16-19)**

Immonen discloses each party (i.e. 1<sup>st</sup> & 2<sup>nd</sup> peers) independently calculates a shared secret key where client A (2<sup>nd</sup> peer) obtains server B's public key (of 1<sup>st</sup> certificate) to calculate a (1<sup>st</sup>) shared secret key (col.1, lines 57-60 and col.3, lines 23-26). Immonen also calculates the same process for the (2<sup>nd</sup>) shared secret key for server B (1<sup>st</sup> peer) so that each party can verify its peer's identity. Thus, Immonen

includes a 1<sup>st</sup> shared secret key for the 2<sup>nd</sup> peer and a 2<sup>nd</sup> shared secret key for the 1<sup>st</sup> peer. However, Immonen does not include the 2<sup>nd</sup> shared secret key is generated with the 2<sup>nd</sup> public key from the 2<sup>nd</sup> peer and a private key of the 1<sup>st</sup> peer.

To simplify terminology from one art to another that corresponds to the claimed invention, is referred in the rejection as follows:

**First peer (1<sup>st</sup> peer) = Server B (Immonen) = Consumer/owner (Moharram)**

**Second peer (2<sup>nd</sup> peer) = Client A (Immonen) = Peer (Moharram)**

Moharram discloses the consumer (1<sup>st</sup> peer) obtains a digital certificate that contains the consumer's public key that is sent to peer (2<sup>nd</sup> peer) and computes a shared secret key (col.9, lines 30-33). Moharram discloses computing the shared secret key from peer's public key and owner private key where owner is referring to the consumer (1<sup>st</sup> peer) (col.9, lines 36-45). Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to modify Immonen to teach generating a 2<sup>nd</sup> shared secret key for the 1<sup>st</sup> peer with the 2<sup>nd</sup> public key from the 2<sup>nd</sup> peer and a private key of the 1<sup>st</sup> peer because this shows that the claimed 1<sup>st</sup> and 2<sup>nd</sup> shared secret key are two separate different shared secret keys that are not generated the same as one another and verifies the parties' identities which certifies the key is his/her own (Moharram-col.9, lines 6-35).

**As per claim 58: See Immonen on col.1, lines 47-67 and col.4, lines 1-5;**

discussing the computer storage medium of claim 57 wherein both the first certificate including the plurality of first parameters and the second certificate including the plurality

of second parameters are generated independently of the first peer and the second peer.

**As per claim 59:** See Immonen on col.3, lines 44-45; discussing the computer storage medium of claim 57 wherein both the first certificate and the second certificate comprise Digital Signature Algorithm (DSA) type certificates.

**As per claim 60:** See Immonen on col.4, lines 1-5; discussing the computer storage medium of claim 57 wherein the plurality of first parameters and the plurality of second parameters comprise digital signature standard parameters.

**As per claim 61:** See Immonen on col.4, lines 44-52; discussing the computer storage medium of claim 57 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

**As per claim 62:** See Immonen on col.4, lines 44-52; discussing the computer storage medium of claim 57 wherein the first peer and the second peer communicate over a network that comprises at least one of a wireless network or a Bluetooth network.

**As per claim 63:**

Immonen discloses a method for generating shared keys comprising:

providing a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters that comprises a first public key for the first peer;

**(col.1, lines 48-51; 1<sup>st</sup> peer is in form of server B)**

generating a second public key by the second peer with at least one parameter of the plurality of first parameters and a first private key of the second peer; **(col.1, lines 54-55 and col.1, line 64-col.2, line 5; 2<sup>nd</sup> peer is in form of client A)**

providing the generated second public key from the second peer to the first peer;

**(col.1, lines 54-55 and col.3, lines 16-25)**

generating a first shared secret key for the second peer with the first public key of the first certificate; and **(col.1, lines 57-60 and col.3, lines 23-26)**

generating a second shared secret key for the first peer [*with the second public key from the second peer and a private key of the first peer*], **(col.1, lines 57-60 and col.3, lines 16-19)**

wherein generating the first shared secret key for the second peer with the first public key of the first certificate is carried out independently of any public key generated by the first peer and the second peer. **(col.1, lines 57-67 and col.3, lines 35-40)**

Immonen discloses each party (i.e. 1<sup>st</sup> & 2<sup>nd</sup> peers) independently calculates a shared secret key where client A (2<sup>nd</sup> peer) obtains server B's public key (of 1<sup>st</sup> certificate) to calculate a (1<sup>st</sup>) shared secret key (col.1, lines 57-60 and col.3, lines 23-26). Immonen also calculates the same process for the (2<sup>nd</sup>) shared secret key for server B (1<sup>st</sup> peer) so that each party can verify its peer's identity. Thus, Immonen includes a 1<sup>st</sup> shared secret key for the 2<sup>nd</sup> peer and a 2<sup>nd</sup> shared secret key for the 1<sup>st</sup> peer. However, Immonen does not include the 2<sup>nd</sup> shared secret key is generated with the 2<sup>nd</sup> public key from the 2<sup>nd</sup> peer and a private key of the 1<sup>st</sup> peer.

To simplify terminology from one art to another that corresponds to the claimed invention, is referred in the rejection as follows:

**First peer (1<sup>st</sup> peer) = Server B (Immonen) = Consumer/owner (Moharram)**

**Second peer (2<sup>nd</sup> peer) = Client A (Immonen) = Peer (Moharram)**



Moharram discloses the consumer (1<sup>st</sup> peer) obtains a digital certificate that contains the consumer's public key that is sent to peer (2<sup>nd</sup> peer) and computes a shared secret key (col.9, lines 30-33). Moharram discloses computing the shared secret key from peer's public key and owner private key where owner is referring to the consumer (1<sup>st</sup> peer) (col.9, lines 36-45). Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to modify Immonen to teach generating a 2nd shared secret key for the 1<sup>st</sup> peer with the 2<sup>nd</sup> public key from the 2<sup>nd</sup> peer and a private key of the 1<sup>st</sup> peer because this shows that the claimed 1<sup>st</sup> and 2<sup>nd</sup> shared secret key are two separate different shared secret keys that are not generated the same as one another and verifies the parties' identities which certifies the key is his/her own (Moharram-col.9, lines 6-35).

### ***Conclusion***

**4. THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Leynna T. Truvan whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/L. T. T./  
Examiner, Art Unit 2435  
/Kimyen Vu/  
Supervisory Patent Examiner, Art Unit 2435